



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/748,406

12/29/2003

Bo-Heung Chung

51876P554

7550

8791

7590

05/17/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN

12400 WILSHIRE BOULEVARD

SEVENTH FLOOR

LOS ANGELES, CA 90025-1030

EXAMINER

PALIWAL, YOGESH

ART UNIT

PAPER NUMBER

2109

MAIL DATE

DELIVERY MODE

05/17/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/748,406

Applicant(s)

CHUNG ET AL.

Examiner

Yogesh Paliwal

Art Unit

2109

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- 1) ☒ Certified copies of the priority documents have been received.
 - 2) ☐ Certified copies of the priority documents have been received in Application No. ____.
 - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 02/11/2004.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: ____.

DETAILED ACTION

Priority

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Specification

2. The disclosure is objected to because of the following informalities:

In page 15-line 22, "wither" should be replaced with "whether".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2 and 7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 7 recites limitations equivalent to claim 2. Because the issues are all the same, claim 2 will be used to exemplify the rejection. Claim 2 depends from claim 1, and step B of claim 1 recites:

"changing the replica of the intrusion detection rule according to a request of
changing the intrusion detection rule from the kernel area"

and step C recites:

Art Unit: 2109

“changing a currently applied intrusion detection rule by exchanging a value of a pointer representing the intrusion detection rule with a value of a pointer representing the changed replica of the intrusion detection rule.”

At this point, after exchanging the pointers, changed replica of the intrusion detection rule is pointing to the currently applied updated intrusion detection rule.

Further claim 2 recites:

“changing again the replica of the intrusion detection rule identically to the currently applied intrusion detection rule”

Above limitation is confusing because replica has already been changed in claim 1, step B, and there was only one replica created in claim 1, step A. So it is confusing as to which replica claim 2 is referring to, and if claim 2 is referring to “changed replica” then as stated above, changed replica of the intrusion detection rule infect is pointing to the currently applied intrusion detection rule after exchanging the pointers (Claim 1, step C). It appears that claim 2 as written is calling to change something to itself. As a result examiner failed to understand the limitations of the claim. The art rejection of above claims will be based on the examiner’s best interpretation of claims.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2109

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-4, 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Marron (US 5359730) in view of Ko (US 7024694)

Regarding **Claims 1 and 6**, Marron discloses method and the inherent corresponding computer program for dynamically changing software module in a kernel level, the method comprising the steps of:

- a) generating a replica of the old program in a kernel area (**Column 6, lines 50-55**);
- b) changing the replica of the software according to a request of changing the software from the kernel area (**Column 6, lines 50-55**); and
- c) changing a currently applied software by exchanging a value of a pointer representing the software with a value of a pointer representing the changed software. (**Column 8, lines 49-52**)

Marron discloses a method of dynamically making software changes in a running system, however he does not teach dynamically changing an intrusion detection rule in a running system.

However, Ko, in the same field of endeavor of intrusion detection at kernel level, discloses that kernel level intrusion detection was well known in the art at the time applicant's invention was made (Column 1, lines 16-21)

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to apply the method of Marron to dynamically update kernel level intrusion detection rules of Ko *to non-disruptively install new versions of operating system [intrusion detection rules] modules while the system is running and one or more processes are executing which use and access such modules* (Marron, Column 5, lines 25-55)

Regarding **Claims 2 and 7**, the rejection of claims 1 and 6 is incorporated and further combination of Marron and Ko discloses a step of changing again the replica of the intrusion detection rule [software module] identically to the currently applied intrusion detection rule [currently applied updated software](**Marron, Column 6, lines 50-55 and Column 8, lines 49-52**);

Regarding **Claims 3 and 8**, the rejection of claims 1 and 6 is incorporated and further Marron discloses in the step b) and the step c), a change state of the intrusion detection rule [software] with a pre-assigned global variable is shown and the intrusion detection rule [software] is changed according to the pre-assigned global variable (**Marron, Column 5, lines 35-41**)

Regarding **Claims 4 and 9**, the rejection of claims 3 and 8 is incorporated and further combination of Marron and Ko discloses that the kernel area transfers the request of changing the intrusion detection rule [updating the software] from the user area by using a system call (**Marron, Column 7, lines 25-28**)

Claims 5 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Marron (US 5359730) and further in view of Stoica (PHD thesis, "Stateless Core: A scalable Approach for Quality of Service in the Internet, Publication date: 12/15/2000)

Regarding **Claims 5 and 10**, the rejection of claims 3 and 8 is incorporated and further combination of Marron and Ko discloses that the kernel area transfers the intrusion detection result (**Ko, Fig. 1, Numeral 105**) to an application program of a host, in which the kernel operates, and/or an external host and/or an external network, the intrusion detection rule being applied to the intrusion detection result (**Ko, Column 2, lines 16-20**).

The combination of Marron and Ko does not disclose that the intrusion detection result being transferred by setting the global variables inside the kernel and determining the transferring position inside the kernel.

However, Stoica, in the same field of endeavor of kernel level monitoring system discloses that the kernel area transfers the kernel-monitoring log by setting the global variables inside the kernel and determining the transferring position inside the kernel (**Page 139, lines 19-21, "To minimize the monitoring overhead, we use the ip_output function call to send this information directly from kernel to an external monitoring machine."**)

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to send the intrusion detection results of the Marron and Ko combination from kernel to an external device by setting the global variables inside the

Art Unit: 2109

kernel and determine the transferring position inside the kernel, as taught by Stoica, to *minimize the monitoring overhead and it also avoids unnecessary context switching between the kernel and the user level (Stoica, Page 139, lines 19-21)*

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Allen et al. (US 5634058): Discloses system for automatically loading kernel modules in a running kernel.
- Shinichi (JP 2000-293362): Discloses a method and system for dynamically changing and correcting configuration of OS kernel code.
- Akgul et al. (US 2003/0074487 A1): Discloses Linking or a new or updated module to an operating system without affecting other modules and without reboot or recompilation.
- Shearer, Jr. et al. (US 6,272,519 B1): Discloses a method to dynamically alter the availability of characteristics of specified system resources. This system allows the modification of system resources without the need to rebuild and re-initialized the operating system. If required by the specific alteration being performed, creation of new kernel control structures may require that one or more of a kernel's static-type data structures be converted to dynamic-type data structures.

Art Unit: 2109


- Roth et al. (US 2002/0023311 A1): discloses a method and apparatus for dynamically updating kernel parameters, which is persistent and lasts across reboots. This system provides a dynamic kernel tunable framework for changing tunable in a kernel without rebooting.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian P. Werner can be reached on (571) 272-7401. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP
5/9/07


BRIAN WERNER
SUPERVISORY PATENT EXAMINER